REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 10-03-2011	2. REPORT TYPE Master of Military Studies Research Paper	3. DATES COVERED *(From - To)* September 2010 - April 2011

4. TITLE AND SUBTITLE Implementing a Modern Warfighting Supply-Chain For Information Technology Acquisitions	5a. CONTRACT NUMBER N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A
6. AUTHOR(S) Rideout, Brian, T.	5d. PROJECT NUMBER N/A
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068	8. PERFORMING ORGANIZATION REPORT NUMBER N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSOR/MONITOR'S ACRONYM(S) N/A
	11. SPONSORING/MONITORING AGENCY REPORT NUMBER N/A

12. DISTRIBUTION AVAILABILITY STATEMENT
Unlimited

13. SUPPLEMENTARY NOTES
N/A

14. ABSTRACT
The Federal Government has committed hundreds of billions of dollars toward solving problems identified in the 9/11 Commission Report, specifically the collective failure to share information and deliver actionable intelligence. The Armed Forces suffered the effects of this dilemma for years in Iraq and Afghanistan and the information-sharing challenge persists. As numbers of sensors and data volumes continue to grow exponentially, it will become more daunting unless the government alters its approach. The DoD must implement a separate, agile process for acquiring IT systems that comprise the majority of ISR functionality. This paper summarizes findings across the DoD that support these assertions as well as subsequent organizational corrective responses. Between a DSB Task Force, OSD, and OMB, a shared set of solutions emerges. These recommendations coincide with the vision set forth in the Marine Corps ISR Enterprise Roadmap. The pairing between the need to revamp IT acquisitions and a service-level volition to improve the process provides a unique opportunity for the Marine Corps to demonstrate success through a service-sponsored pilot program.

15. SUBJECT TERMS
Agile Acquisitions, Information Technology, Marine Corps Intelligence Surveillance Reconnaissance Enterprise, Product Line Architecture, Automated Requirements Generation, Certification and Accreditation, Information Assurance Range.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 34	19a. NAME OF RESPONSIBLE PERSON Marine Corps University / Command and Staff College
a. REPORT Unclass	b. ABSTRACT Unclass	c. THIS PAGE Unclass			19b. TELEPONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

IMPLEMENTING A MODERN WARFIGHTING SUPPLY-CHAIN FOR
INFORMATION TECHNOLOGY ACQUISITIONS
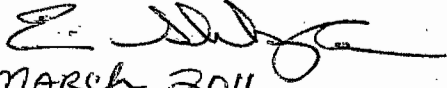
SUBMITTED IN PARTIAL FILFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

MAJOR BRIAN T. RIDEOUT

AY 10-11

Mentor and Oral Defense Committee Member: Dr. Eric Y. Shibuya, PhD
Approved: _____
Date: *10 MARCH 2011*

Oral Defense Committee Members: Dr. Jonathan Phillips, PhD, LTC Michael Lewis, USA
Approved: _____
Date: 10 March 2011

EXECUTIVE SUMMARY

Title: Implementing A Modern Warfighting Supply Chain for Information Technology (IT) Acquisitions

Author: Major Brian Rideout, United States Marine Corps

Thesis: The Department of Defense (DoD) must implement a separate, agile process for acquiring Information Technology systems that comprise the majority of Intelligence, Surveillance, and Reconnaissance (ISR) functionality.

Discussion: The Federal Government has committed hundreds of billions of dollars toward solving problems identified in the 9/11 Commission Report, specifically the government's failure to share information and deliver timely, actionable intelligence. Members of the Armed Forces experienced the effects of this dilemma for years in Iraq and they continue to feel its effects in Afghanistan. The challenge will only increase unless the government alters its approach.

   The constant evolution of IT provides opportunities for continuous improvement; however, new IT procurement is governed by the same acquisition process used to obtain material like tanks and aircraft carriers. This course moves too slowly to keep pace with the rapid advances in IT. The government needs an entity committed to fixing the process with a vision to establish and implement a disciplined, incremental, and continuous value delivery chain from both operational and acquisition perspectives. Practical and swift delivery of today's best IT into the hands of war-fighters should guide this organization in every action. Policy changes and paradigm shifts that facilitate synchronizing requirements, resources, and acquisition management are necessary to achieve success. Corresponding shifts at middle management layers are equally critical.

Conclusion: In reviewing findings across the DoD as well as subsequent responses to the Defense Science Board (DSB) Task Force Report on the need to revamp IT Acquisitions, a shared set of solutions emerges. These recommendations align with the recently signed Marine Corps' ISR Enterprise Roadmap. Joining (1) the government's need to revamp IT acquisitions and (2) a service-level volition to derive value from improved processes, provides a unique opportunity for the Marine Corps Intelligence Enterprise to demonstrate success through a service-sponsored pilot program. A new model that implements a modern war-fighting supply chain for IT acquisitions provides a systematic approach to achieve this end.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE
INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE
VIEWS OF EITHER THE MARINES CORPS COMMAND AND STAFF COLLEGE OR ANY
OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD
INCLUDE THE FOREGOING STATEMENT.

QUOTATIONS FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY
PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER
ACKNOWLEDGEMENT IS MADE.

LIST OF ILLUSTRATIONS

LIST OF TABLES

LIST OF ACRONYMS

C&A	Certification and Accreditation
CCE	Common Computing Environment
CIO	Chief Information Officer
CMC	Commandant of the United States Marine Corps
COTS	Commercial-off-the-shelf
DC, CD&I	Deputy Commandant, Combat Development Integration
DCGS	Distributed Common Ground System
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DIRINT	Director of Intelligence
DoD	Department of Defense
DSB	Defense Science Board
ERP	Enterprise Requirements Plan
FY	Fiscal Year
IA	Information Assurance
IAVA	Information Assurance Vulnerability Assessment
IDU	Intelligence Dissemination & Utilization
ISIL	Intelligence System Integration Laboratory
ISR	Intelligence, Surveillance, Reconnaissance
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
JROC	Joint Requirements Oversight Council
MCISR-E	Marine Corps ISR - Enterprise
MCSC	Marine Corps Systems Command
MCSCP	Marine Corps Service Campaign Plan
OSD	Office of the Secretary of Defense
OMB	Office of Management and Budget
ONR	Office of Naval Research
PISR	Persistent ISR
PLA	Product Line Architecture
QA	Quality Attribute
RAP	Resource Allocation Process
S&T	Science and Technology
SECDEF	Secretary of Defense
SIDECAR	Semantically Informed Dynamic Engineering of Capabilities and Requirements
T&E	Testing and Evaluation
TF	Task Force
TRL	Technology Readiness Level

TABLE OF CONTENTS

STANDARD FORM (SF) 298

REPORT DOCUMENTATION PAGE		FORM APPROVED --- OMB NO. 0704-0188	
PUBLIC REPORTING BURDEN FOR THIS COLLECTION OF INFORMATION IS ESTIMATED TO AVERAGE 1 HOUR PER RESPONSE, INCLUDING THE TIME FOR REVIEWING INSTRUCTIONS, SEARCHING EXISTING DATA SOURCES, GATHERING AND MAINTAINING THE DATA NEEDED, AND COMPLETING AND REVIEWING THE COLLECTION OF INFORMATION. SEND COMMENTS REGARDING THIS BURDEN ESTIMATE OR ANY OTHER ASPECT OF THIS COLLECTION OF INFORMATION, INCLUDING SUGGESTIONS FOR REDUCING THIS BURDEN, TO WASHINGTON HEADQUARTERS SERVICES, DIRECTORATE FOR INFORMATION OPERATIONS AND REPORTS, 1215 JEFFERSON DAVIS HIGHWAY, SUITE 1204, ARLINGTON, VA 22202-4302, AND TO THE OFFICE OF MANAGEMENT AND BUDGET, PAPERWORK REDUCTION PROJECT (0704-0188) WASHINGTON, DC 20503			
1. AGENCY USE ONLY (LEAVE BLANK)	2. REPORT DATE *10 MARCH 2011*	3. REPORT TYPE AND DATES COVERED *STUDENT RESEARCH PAPER*	
4. TITLE AND SUBTITLE: *IMPLEMENTING A MODERN WARFIGHTING SUPPLY-CHAIN FOR INFORMATION TECHNOLOGY ACQUISITIONS*		5. FUNDING NUMBERS N/A	
6. AUTHOR(S) *MAJOR BRIAN RIDEOUT, USMC*			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) *USMC COMMAND AND STAFF COLLEGE 2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068*		8. PERFORMING ORGANIZATION REPORT NUMBER *NONE*	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) *SAME AS #7.*		10. SPONSORING/MONITORING AGENCY REPORT NUMBER: *NONE*	
11. SUPPLEMENTARY NOTES *NONE*			
12A. DISTRIBUTION/AVAILABILITY STATEMENT *NO RESTRICTIONS*		12B. DISTRIBUTION CODE *N/A*	

ABSTRACT:

The Federal Government has committed hundreds of billions of dollars toward solving problems identified in the 9/11 Commission Report, specifically the collective failure to share information and deliver timely, actionable intelligence. Members of the Armed Forces suffered the effects of this dilemma for years in Iraq and continue to suffer in Afghanistan. Notwithstanding the investment to date, the information-sharing challenge persists. As numbers of sensors and data volumes continue to grow exponentially, it will become more daunting unless the government alters its approach. The DoD must implement a separate, agile process for acquiring IT systems that comprise the majority of ISR functionality.

This paper summarizes findings across the DoD that support the above assertions as well as subsequent organizational corrective responses. Between a DSB Task Force, the Office of the Secretary of Defense, and the Office of Management and Budget, a shared set of solutions emerges. These recommendations coincide with the vision set forth in a recently signed Marine Corps ISR Enterprise Roadmap. Thus, the pairing between the government's need to revamp IT acquisitions and a service-level volition to improve the process provides a unique opportunity for the Marine Corps Intelligence Enterprise to demonstrate success through a service-sponsored pilot program.

14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH):		15. NUMBER OF PAGES: 34	
		16. PRICE CODE: N/A	
17. SECURITY CLASSIFICATION OF REPORT *UNCLASSIFIED*	18. SECURITY CLASSIFICATION OF THIS PAGE *UNCLASSIFIED*	19. SECURITY CLASSIFICATION OF ABSTRACT *UNCLASSIFIED*	20. LIMITATION OF ABSTRACT

The inability to effectively acquire information technology systems is critical to national security. Thus, the many challenges surrounding information technology must be addressed if DoD is to remain a military leader in the future. [1]

Introduction

The Federal Government has committed hundreds of billions of dollars toward solving

problems identified in the 9/11 Commission Report, specifically the government's collective failure to

share information and deliver timely, actionable intelligence. Members of the Armed Forces suffered

the effects of this dilemma for years in Iraq and continue to suffer in Afghanistan. Notwithstanding the

investment to date, the information-sharing challenge persists. As numbers of sensors and data

volumes continue to grow exponentially, it will become more daunting unless the government alters its

approach. The DoD must implement a separate, agile process for acquiring IT systems that comprise

the majority of ISR functionality.

Current processes for collecting and disseminating actionable intelligence as well as the

processes for acquiring the necessary enabling technology are broken. The government needs a

champion committed to fixing both at the same time. This champion-entity will implement a

disciplined, incremental, and continuous value delivery chain of both operationally critical, actionable

intelligence, and the rapidly evolving technological tools necessary to that end. Synchronizing

requirements, resources, and acquisition management to support this new agile model requires that

stakeholders' current methods and mindsets change, especially at the middle management layer(s).

To develop a feasible solution, this paper summarizes findings across the DoD that support the

above assertions as well as subsequent organizational corrective responses. Between a DSB Task

Force, the Office of the Secretary of Defense (OSD), and the Office of Management and Budget

(OMB), a shared set of solutions emerges. These recommendations coincide with the vision set forth in

a recently signed Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E)

Roadmap.[2] Thus, the pairing between (1) the government's need to revamp IT acquisitions and (2) a

service-level volition to derive value from improved processes provides a unique opportunity for the Marine Corps Intelligence Enterprise to demonstrate success through a service-sponsored pilot program. This paper provides a credible, systematic model to achieve this end and concludes with recommendations for further development.

Background: Defense Science Board Task Force Findings

The fundamental problem DoD faces is that the deliberate process through which weapons systems and IT are acquired does not match the speed at which new IT capabilities are being introduced into today's information age.[3]

In March 2009, the DSB Task Force (TF) submitted findings to Congress regarding the process DoD uses to acquire IT. Several ideas emerged supporting the conclusion that a new acquisition process should be developed for IT in order to account for the increasingly critical position IT plays in DoD warfare systems. Proposed changes must accommodate the rapid growth rate of IT and answer the evolving, urgent needs of the war-fighter.[4] Underlying themes supporting a new process include an emphasis on time, requirements, architecture, leadership and policy, security, and cost. A succinct review of each area follows.

Time

In 1965, Intel co-founder Gordon Moore projected the number of transistors on an integrated circuit board would double every two years.[5] Since then, the application of "Moore's Law" has expanded to processing speed, memory capacity; "even the number and size of pixels in digital cameras"[6] (see Figure 1, Appendix A). The hardware and software components that deliver this type of IT functionality comprise the essence of almost every ISR system employed today. Retaining an edge on an adaptive, informed adversary thus requires an ability to inject new IT capabilities on pace with the proven rate of technological change. That requirement places significant pressure on acquisition professionals bound by an antiquated process.

The conventional DoD acquisition process is "too long and cumbersome to fit the needs of many IT systems which require continuous changes and upgrades driven by the short half-life of commercial IT"[7] (see Figure 2, Appendix A). The overall portfolio of DoD IT programs has experienced a twenty-one month delay in delivering initial operating capability (IOC) to the war-fighter and 12% are more than four years late.[8] Further studies of major automated information systems acquisitions concluded that the average time to deliver initial program capability took ninety-one months.[9] Following Moore's Law, this equates to missing roughly four doublings of technological capacity. Clearly, a rapid IT acquisition process is necessary if the DoD intends to harvest value from the high-speed cycle of continuously improving IT.

The DoD lags in a world driven by [commercial] organizations operating on six to twelve month development cycles and technology generations of twelve to twenty-four months.[10] Cycle time to deliver increased value to the warfighter should therefore ascend to the top of the DoD's priorities. The new process should be "agile and geared toward delivering meaningful increments of capability in approximately eighteen months or less."[11] These increments should be prioritized through iterative requirements reviews and frequent assessments of technical readiness. The first step in accomplishing the eighteen-month objective requires a significant overhaul of the requirements process.

Requirements

In early 2009, Secretary of Defense (SECDEF) Robert Gates publicly criticized the deliberate acquisitions process: "The DoD's conventional modernization programs seek a 99% solution over a period of years. Stability and counterinsurgency missions require 75% solutions over a period of months. The challenge is whether these two different paradigms can be made to coexist in the military's mindset and bureaucracy."[12] The SECDEF calls for well-defined initial objectives rather than over-defined final requirements in order to deliver capability increments. This approach enables requirements to evolve in a manner that allows for "desired capabilities to be traded-off against cost

and IOC in order to deliver the best capability to the field in a timely manner."[13] This modular

approach exploits technology readily available in the commercial sector. The method, sometimes

called "open-systems"[14] does not ignore the final 25% of the solution. Rather, it allows for planned

capability improvements without withholding less complete solutions from the warriors who need

them now.

Instituting a modular, open-systems requirements methodology includes many advantages and

a few demands. Regarding the latter, end-users must remain actively engaged and apply the necessary

analytical rigor throughout the process from conception through delivery and feedback phases.

Requirements must be constructed in a context that looks across the spectrum, or enterprise of systems

as opposed to disparate analyses of multiple systems. Obtaining such a holistic perspective demands

significant design changes in order to account for technology growth and dynamic circumstances.[15] By

concentrating on manageable increments that deliver capabilities in shorter time frames, these

adjustments will speed the process, increase the likelihood of repeated success, and reduce risks to

cost, schedule, and performance.[16]

Architecture

Defining what architecture is presents a challenge. The fact that Carnegie Mellon's Software

Engineering Institute website provides over sixty explanations[17] accounts for much of the confusion.

The DSB TF echoed this sentiment claiming, "Architecture is too often viewed as a paper exercise

rather than a model-driven, analytically supported, and rigorous engineering process incorporating

enterprise-wide considerations for functionality and interface definition."[18]

A simpler definition, in the context of IT, consists of a plan for assembling things based on a

framework for integrating components. This explanation of [software] architecture potentially offers

answers to questions such as, "How can one economically reuse things? Or, how does one improve

part of something without starting from scratch?"[19] In this sense, software architecture models natural

selection by "fostering processes for fixing or changing broken parts while keeping and enhancing remaining components. This reuse of suitable components reinforces selection and improvement which caters to an evolutionary approach."[20] If one can invest, develop, and maintain an architecture that evolves with the actual pace of technological change, then that architecture will provide value without incurring costly rewrites or schedule delays.

The DSB report acknowledged that in a net-centric world, "IT systems exist in shared IT environments with more and more IT systems being constructed from common components."[21] The benefits of this natural selection approach include more rapid development, increased reuse of components, and survivability; however, the potential for increased complexity, interdependencies, and new vulnerabilities also exists.[22] By tackling small increments of capability in an evolutionary, iterative fashion, acquisitions professionals can mitigate complexity risks and seize opportunities to accelerate development through proven [software] components. Additional benefits of this method include: frequent opportunities to identify and address system interoperability issues; the option to integrate new technologies as they become available to support development; and the ability to deliver improved mission capabilities through each technology iteration.[23]

Leadership and Policy

In 1996, the DoD made a serious attempt to improve the way Federal agencies acquire IT and shorten acquisition cycle time. Although the Clinger-Cohen Act of 1996 was well intentioned, misinterpretation inadvertently forced program managers to comply with bureaucratic burdens that hindered the ability to execute swiftly without adding value. Several attempts to improve the process have followed, including the newly modified DoD Instruction 5000.02 acquisition policy designed "to add more rigor and discipline in the early part of the acquisition process."[24] One problem with these shifts in policy remains their collective focus on a "one-size-fits-all" model for both major automated information systems and major defense acquisition systems.[25] Another problem is the reality that

adding bureaucracy rarely streamlines the process. Consequently, the DSB strongly supports a unique acquisition system for IT.

DoD systems have experienced a sharp increase in their reliance on software. In 1970, software accounted for 20% of weapon systems functionality as compared to 80% in 2000. Today, over 90% of a system's functionality comes from software.[26] The latest Defense Acquisitions Guidebook appears to account for this trend as it places considerable attention on how to acquire this functionality. Out of 929 pages, 186 pages, or roughly 20% of the document, are dedicated solely to IT acquisition.[27] However, despite current guidance, IT programs continue to experience significant delays.

A review of major IT acquisition programs revealed three root causes behind the schedule and performance issues. First, senior leaders lack technical experience and understanding; second, Program Executive Officers and Program Managers also lack requisite [IT] experience; and third, the acquisition process is too bureaucratic.[28] While easy to blame the institution, one must not overlook the people executing the process. A generic top-down approach coupled with poor management has continually failed to deliver value in a timely manner. In the end, all this hinders the warfighter's ability to acquire and use IT to improve situational awareness, facilitate collaboration across the battlespace, and support rapid decision-making.[29] Any further shifts in policy should therefore be complimented by new models and corresponding incentives to ensure the people in charge understand and execute the changes.

Security

The DSB concluded that the DoD's "inability to effectively acquire IT systems is critical to national security" and that the United States must tackle the challenges surrounding IT acquisition if it expects to remain a military leader in today's world.[30] The Task Force attributed this "inability" to the constraints of a single, deliberate process. Whether one attributes failure to process, policy, or people, the fact remains that today's information age offers potential adversaries unlimited access to acquire

the same [commercial] technologies available to the U.S.[31] This type of open, global availability presents unique concerns, especially when one considers that our non-state adversaries are not encumbered by bureaucratic, complex acquisitions processes.

The exponential growth in technology carries significant trade-offs, e.g., the cost of staying in front of adversaries vs. the vulnerability posed by increasing amounts of software.[32] Currently, the U.S. enjoys the most capable defense systems in the world including its command and control, decision support, and situational awareness systems. At the heart of each of these examples, IT represents a critical component. As capabilities change and threats evolve, these systems will require upgrades and/or technology refreshes. Further, the DoD Information Assurance Certification and Accreditation Process (DIACAP) mandates applying a stringent risk management approach before systems are authorized to connect to various DoD networks.[33] By itself, this process can add up to one year or more (see Figure 3, Appendix A). Adhering to extant policies under current technology growth rates thus widens the gap between the latest IT capabilities and the DoD's ability to certify them. This brings us to the final factor of cost.

Cost

Probably the most significant and controversial issue associated with a new process is cost. In an effort to mitigate subjectivity or accusations of manipulating math, cost will not be viewed independently. Instead, cost will be placed in the context of aforementioned trends such as the increasing reliance on software in DoD systems. The DSB discovered that maintaining the annual cost of DoD's software-enabled capabilities could rise at ten times the cost of similar capabilities "provided by the established and structured commercial software industry."[34] These two trends highlight an important decision point. The DoD can spend ten times more on components whose demand is on the rise, or the Federal Government can achieve a better return on investment without sacrificing capability, by fully embracing commercial-off-the-shelf (COTS) technology.

Federal budget trends also reinforce the DoD's increasing dependence on IT. In fiscal year (FY) 2007, the DoD invested approximately $30.5 billion[35] on IT systems whereas in FY 2011, that figure grew to $36.3 billion.[36] Given the current economic climate, there is pressure to cut, not increase spending. Fortunately, there is another option. Rather than grow the IT budget by nearly 20%, the government could maintain a constant budget and provide more value per dollar spent. The fact that "the majority of commercial code has grown exponentially while the cost remains nearly constant"[37] supports such an approach. A more or less constant outlay returns considerably more value over time as technology evolves. Achieving such economic returns is attributed to commercial standards and processes that help the commercial sector reuse valued [software] components. In particular, use of modular, open standard, Product Line Architecture (PLA) to create a persistent plug-and-play IT "platform" allows extremely efficient re-use and enables lucrative time-to-value for multiple IT-enabled enterprises.[38] These commercial "best practices" represent an intersection of COTS speed, architecture, and cost, each of which should be considered in context with the others.

Responses to the Problem: OSD and U.S. Chief Information Officer

The traditional acquisition process used to develop and acquire military technology is not aligned with the speed, agility, and adaptability at which new IT capabilities are introduced in today's information age.[39]

Approximately six months after the DSB TF published its findings, Congress passed the National Defense Authorization Act for FY2010. Section 804 of this Act tasked the SECDEF with developing and implementing a "New Acquisition Process for Information Technology Systems" based on recommendations from the March 2009 DSB report. This section also recommended including: "(A) early and continual involvement of the user; (B) multiple, rapidly executed increments or releases of capability; (C) early, successive prototyping to support an evolutionary approach; and (D) a modular, open-systems approach."[40] OSD and the U.S. Chief Information Officer (CIO), under OMB,

provided responses in November and December 2010, respectively. A summary of their findings follows.

Time

OSD's "New Approach for Delivering IT Capabilities in the DoD" acknowledges the need to shorten project initiation timelines in order to respond to the dynamic IT environment.[41] Similarly, the U.S. CIO's "25 Point Implementation Plan to Reform Federal IT Management" identifies timelines and project scope as two of the most consistent problems contributing to the Federal IT Acquisition challenge. The U.S. CIO found that many current IT projects "are scheduled to produce their first deliverables years after work begins, in some cases up to six years later."[42] OSD suggests "fostering an environment for mission-focused, time-critical deliveries by moving from large, multi-year programs to short-duration projects that deliver incremental capabilities in shorter timeframes."[43]

Keen awareness of rapid technology change rates led to the CIO's recommendation that "Federal IT programs be structured to deploy working business functionality in release cycles no longer than twelve months with initial deployment to end users no later than eighteen months after a program begins."[44] That timetable is attainable but it will require project oversight with "more accountability on timely coordination, agile, yet informed, decision cycles, and increased stakeholder involvement through more frequent reviews."[45] The single goal here is to deliver functionality to the user at a faster pace. In short, DoD needs to shift its current acquisitions approach to one that permits smaller, successive capabilities that will reach an intended customer base prior to becoming obsolete.

Requirements

The generation and management of system requirements must be swift and flexible in order to account for the uncertainty of today's dynamic environment. Historically, IT requirements have been "hindered by inadequate communication with industry."[46] Too often, problems also stem from insufficient communication between the program staff and the end users of the system. Disconnects

like these lead to ill-defined or poorly written contracts which result in waste, schedule delays, and an "erosion of the value of IT investments."[47] Unfortunately the problem, though clear, does not lend itself to an obvious solution.

OSD and OMB concur on the DSB findings that user involvement, a modular open systems approach, and capability delivered in manageably-small increments comprise the necessary focal points in this category. OSD adds that an "enterprise focus across the portfolio of capabilities with established standards and open, modular platforms vice customized solutions, will ensure interoperability and seamless integration."[48] When done efficiently, requirements should be defined at a high [enterprise] level, regularly refined and prioritized by an active group of stakeholders, assessed by technical experts, and pushed out as increments to end users. If certain functionalities are not yet mature or do not meet a specified priority cut-off, then they should be deferred to future increments.[49] Employing this disciplined approach prevents the temptation to constantly add requirements and avoids delivering non-critical functionality.

In response to the DSB Study, the Joint Staff Deputy Director for Resources and Acquisition proposed the Joint Capabilities Integration and Development (JCIDS) "IT Box" in order to ensure that IT programs "have the appropriate flexibility and oversight to plan for and incorporate evolving technology."[50] OSD praised this streamlining initiative citing several advantages. These include: (1) less return trips to high level review and validation boards such as the Joint Requirements Oversight Council (JROC); (2) the ability to delegate authority for incremental upgrades; and (3) the potential for multiple projects to be derived from a single Capabilities Development Document.[51] This revolutionary approach replaces the prolonged process of program phases, milestone, and program reviews depicted in Figure 2 and replaces it with a process that better facilitates incorporating the evolution of existing capabilities, the initiation of new projects, and the delivery of incremental

capability. The next step towards ensuring this method's success at the enterprise level is implementing the right structure.

Architecture

While the DSB report emphasized faster, incremental delivery of capability that evolves with the rate of technological change, it did not prescribe how to achieve this end. The OSD and OMB responses were equally inconclusive with regard to leveraging architecture successfully. In OSD's report to Congress, the term "architecture" is used twelve times in eight different contexts ranging from technical architecture to enterprise architecture to service-oriented architecture. That leaves readers either confident that all aforementioned types of architecture must be pursued, or confused and left to select for themselves. Conversely, the U.S. CIO mentions the word only once in the "25 Point Implementation Plan." The previous discussion on cost, specifically, the disproportionate economic return the commercial sector enjoys with the help of structure, standards, and component reuse, strongly suggests that the DoD should reexamine the importance of architecture.

The DoD does recognize a common vision for employing architecture. This includes: aligning projects within each broad portfolio to fill common gaps; developing and enforcing information standards that help regulate information definitions; emphasizing compliance; and rationalizing performance requirements.[52] Combining that intent with a modular, open system approach promotes competition by permitting a wider selection of options. It also facilitates delivering capability in an iterative fashion while identifying and eliminating redundant capability.[53] Finally, it facilitates upgrades and encourages commercial vendors to develop non-exclusive interfaces so that the vast array of pre-qualified and already [security] certified IT services can be integrated immediately."[54] All of these advantages should better enable the DoD to take advantage of agile development in order to field current capabilities rapidly.

Leadership and Policy

Lack of experience, poor management, and the need for separate policies comprise major issues when it comes to leadership and policy. OSD and OMB agree that the government has missed out on private sector transformations, due in part to "its poor management of large technology investments."[55] Both agencies also agree that senior leaders need to engage in order to develop and implement reforms. Long-standing cultural mindsets present significant obstacles, especially when it comes to moving from a single delivery to multiple deliveries in an environment that seeks to release deployable capabilities every twelve to eighteen months. According to the U.S. CIO, now is the time for management to focus on these value-added activities.[56]

At the execution level, leaders should embrace recurring in-progress reviews with empowered stakeholders and customers alike. This kind of joint governance increases oversight, enforces accountability, and adds necessary transparency.[57] It also provides the opportunity to address issues pertaining to the project, e.g., execution status, fielding schedules, and budget planning, as well as the customer's involvement, e.g., design feedback, testing, and concept of operations development.[58] In an environment that intends to cycle increments every twelve to eighteen months, these IPRs will tax human resources; however, they must occur for the DoD to achieve the requisite oversight between project leads and appropriate level executives. Structured, frequent, open meetings of this nature also help mitigate potentially unconstructive contributions stemming from middle layer managers.

Security

An incremental, modular approach to IT acquisitions that delivers capability in eighteen months or less necessitates a corresponding shift in DoD's testing and certification methodology. Proposed solutions must address and test security, interoperability, and risk management. A proponent of accelerating this effort, OSD suggests integrating system security requirements with performance requirements in order to "facilitate a complete and total design solution."[59] OSD also recommends

increasing "the use of test automation as well as test infrastructure in a persistent, virtual, service-based environment."[60] Likewise, one of the U.S. CIO's main thrusts is to maximize the use of virtual environments that employ cloud computing models in order to enable multiple, disparate agencies to contribute toward improving security. Cloud computing represents a location independent model that allows unlimited networked users the ability to contribute, consume, or deliver IT services over the Internet.[61] From a security standpoint, the cloud allows customers to "rely on authorizations completed by other agencies" and/or use existing authorizations, so that separate certifications are only completed when "additional, agency-specific requirements" are necessary.[62] The end result will yield consistently shorter timelines and increased efficiency.

Cost

The DoD's primary Resource Allocation Process (RAP) or, Planning, Programming, Budgeting, and Execution, is driven by a calendar, not events. Therefore any changes in time, requirements, etc. must be accompanied by policy changes affecting the RAP. OSD recognizes the need to update this policy. "Current policy for requirements, funding, and acquisition of IT is based on long-standing statutes and regulations using 20th Century protocols and industrial age practices designed principally for custom-developed hardware acquisition."[63] The "New Approach" Report to Congress does caution that emphasizing smaller projects, i.e., manageable increments, could adversely impact DoD's relationship with industry. Specifically, that "smaller efforts may reduce entry barriers for small to mid-sized companies but they also remove the relative business security afforded by larger, longer-term efforts."[64]

The U.S. CIO proposes implementing flexible budget models that support modular development, adopting shared solutions, and delegating fiscal decisions down to the point of execution. Shared solutions comprise light technologies like the previously mentioned cloud computing services. This model follows a "pay-as-you-go" approach, requires low initial investments, and supports

unlimited extensibility as service demands increase.[65] Conversely, it empowers decision makers to cease investing when demands change, thereby optimizing reinvestments for higher priority mission needs. User demand is not always predictable. Thus, in order to deploy IT services timely and successfully, decisions on technology solutions must be made at the execution level.[66] Additionally, ample management reserve funds should be available to address emergent needs. Ironically, the extant procedures that are supposed to control these decisions are the same ones that prevent agencies from achieving the efficiencies described above. The tradeoff is that this increased flexibility will be accompanied by more scrutiny and higher expectations.

Relevance to USMC: MCISR-E as a Pilot Program

For Marine Corps Intelligence to remain effective, it must evolve and adapt to both the changing demands of the modern battlefield and the capabilities provided by advances in technology.[67]

In December 2009, the Commandant of the Marine Corps (CMC) released the Marine Corps Service Campaign Plan (MCSCP) with a vision to maintain proficiency across core competencies and posture the Marine Corps for the future.[68] To achieve that end, the MCSCP integrates the CMC's functional area advocates to support Marine Corps programmatic processes and address Combatant Commander requirements. As the CMC's advocate for intelligence, the Director of Intelligence (DIRINT) responded by promulgating the MCISR-E Roadmap in April 2010 as an appendix to the MCSCP. The MCSIR-E embraces the CMC's integration intent by driving Headquarters, Intelligence Department (I Dept), Deputy Commandant for Combat Development and Integration (DC, CD&I), and Marine Corps Systems Command (MCSC) to "identify, assess, and implement opportunities to align the advocacy, requirements, and acquisition communities"[69] across the three pillars of the MCISR-E. These include: Persistent ISR (PISR), Distributed Common Ground System (DCGS), and Intelligence Dissemination and Utilization (IDU).

The DIRINT's Roadmap provides four focus areas to facilitate the developing and sustaining a fully integrated, adaptive enterprise responsive to new opportunities through 2025 and beyond.[70] Two of these objectives echo previously mentioned challenges (summarized in Table 1, Appendix B). Those objectives include: (1) "integrating all service ISR elements into a holistic system networked across all echelons and functions" and (2) improving process proficiency through continuous, detailed self-assessments.[71] The MCISR-E operating concept suggests fusing these areas to construct such a system through a rapid prototyping and acquisition process.[72] By its nature, prototyping seeks constant feedback on requirements analysis and design decisions from end users; however, instantiating such a process has proven elusive. The following section offers a systematic prototyping process for rapidly identifying, developing, and delivering increments of new technology inside the desired eighteen-month window.

A New IT Acquisition Model for the MCISR-E

A modern IT acquisition supply chain (Figure 4, Appendix A) could enable the MCISR-E to conceive, produce, and deliver increments of IT in eighteen months or less. The model starts by addressing the long, serial progression of static requirements and compliance documents mandated by JCIDS. The MCISR-E envisions an Equipment Transition Plan that establishes new business processes for combat development and acquisitions to include: "developing a common computing environment (CCE), streamlining requirements development, and the ability to remain adaptive and ahead of the critical technology curve."[73] A corresponding Enterprise Requirements Plan (ERP) seeks to meet that intent by employing "a documentation strategy to reduce costs, speed fielding, enhance capabilities, and ensure the integration of funding lines and programs of record."[74] In keeping with the DIRINT's alignment vision, CD&I's Intelligence Integration Division joined MCSC's Rapid Prototyping Team to devise solutions for both plans.

Automated Requirements Generation

The proposed process of codifying MCISR-E requirements would diverge from current practice and develop a suite of machine-readable acquisitions documentation deliberately focused on content over form.[75] The resultant prototype, Semantically Informed Dynamic Engineering of Capabilities and Requirements (SIDECAR), replaces the paper-intensive engineering and documentation process with an automated, parallel approach. SIDECAR employs advanced artificial intelligence to link multiple databases addressing policy, requirements, architecture, technology, and resources.[76] Connections like these enable an intuitively searchable database to transform machine views into readable "snapshots" that depict current states of alternatives, compliance, etc. The main advantage is that SIDECAR hides these complexities behind a simple user interface similar to the way TurboTax software conceals hundreds of pages of tax code.

SIDECAR offers more than another toolset to reduce errors and decrease the amount of time to comply with documentation requirements mandated by the JCIDS. It adds structure through the use of Policy Markup Language. This enables machines to check a document's compliance against hundreds of disparate and sometimes conflicting policies. It also allows users to represent enterprise goals and instantaneously view the relationship of individual program elements to those goals.[77] For example, an analyst poses an ad hoc query on a particular system requirement and receives scenarios of interest related to other systems across the enterprise. This is made possible by SIDECAR's semantically integrated data structure and pattern recognition software. Integrating SIDECAR as an alternative to status quo requirements development will reduce redundant spending, reveal associations between systems, and accelerate the generation of new requirements. Successfully transforming these requirements into material solutions starts with the next entity.

Leveraging Science & Technology (S&T)

The MCISR-E Roadmap calls for developing a bi-annual intelligence S&T strategy to accomplish two things: (1) "Develop short-range 'leap-ahead' technologies within existing intelligence acquisition programs" and (2) "develop longer-term innovative technologies."[78] The Office of Naval Research (ONR) Code 30 ISR Thrust contributes significantly in both capacities by "seeking to develop and leverage advanced technologies for applications in future ISR systems."[79] As an informal agent for the MCISR-E, ONR possesses a unique and mutually beneficial relationship with industry to help close the gap between conceptual requirements and material realities. ONR can issue Broad Agency Announcements inviting COTS IT industry to demonstrate desired capabilities against requirements needs or gaps. Top performing vendors win contracts from these Agency Announcements thereby decreasing the time it takes to satisfy requirements.

In a more formal capacity, ONR should inform the requirements process by continually identifying and validating what [technology] is within the realm of possible. As ONR explores and narrows the field of alternatives, they should methodically assess technology readiness levels[80] (TRL), technical risks, and availability. These inputs would in turn populate SIDECAR's technology database and enable tailored display options (e.g., match COTS sensors with TRL six or higher against Gap X). Frequent collaboration between requirements analysts and S&T engineers will enhance communication with industry and mitigate schedule delays. The interaction should include explicitly defined system interfaces and data standards for the purpose of improving the quality of written technical specifications. It will also encourage competition by offering incentives for industry to invest in and direct internal corporate resources toward developing COTS products that fulfill current gaps.[81]

Product Line Architecture

The three MCISR-E pillars (DCGS, PISR, IDU) offer exceptional opportunities to develop PLAs as interrelated segments of a larger Enterprise Architecture. Based on commercial practices for

modular, open system design, a PLA "is optimized for rapid discovery, development, and fielding of incremental capability."[82] It also provides an extensible structure without compromising adaptation and speed. Further, PLA can achieve the Enterprise's intent to establish a CCE.[83]

In 2010, MCSC developed a prototype PISR PLA to commence realizing that CCE in the context of the first MCISR-E objective: "The synergistic integration of all service ISR elements."[84] Selecting PISR for the first PLA represented "a deliberate departure from a status quo deemed inadequate by USMC leadership to fight modern threats."[85] By concentrating on sensors, platforms that carry or deliver them, and their supporting information systems, the PISR PLA seeks to create a family of interoperable systems capable of being reconfigured for multiple mission environments. This inaugural PLA also offers a foundation from which to cultivate PLAs for DCGS and IDU.

The modern IT acquisition supply chain (Figure 4, Appendix A) suggests a larger role for the architecture entity. In addition to developing a PLA, the Chief Architect collaborates with requirements analysts to ensure standards are clearly articulated to industry. Likewise, the Chief Architect constantly communicates with S&T engineers to anticipate and account for technology trends. Promoting transparency in this manner will lower the barriers that "traditionally impede [the] government's ability to deploy advanced applications, innovative processes, and new generations of computing and communications infrastructure."[86]

An Intelligence System Integration Lab (ISIL) forms the nucleus of the architecture section. The ISIL offers architects and engineers the ability to maintain an evolving "knowledge base" of the PLA. That knowledge base contains a centralized repository of information[87] including types of interfaces, standards, and quality attributes (QA). A QA defines "properties of a work product to be judged by the stakeholders."[88] These characteristics essentially represent those product aspects deemed most important to success because they deliver [expected] results or avoid unacceptable outcomes for the end users.[89] Thus, updating a PLA knowledge base depends on the quality and frequency of inputs

from end users as well as those S&T agents who are connected to an ecosystem of cutting-edge technology vendors. The ISIL weighs QA priorities with developing requirements and offers the ability to conduct simulated operational assessments. These cost-effective examinations can verify functionality against prearranged QAs. They can also reveal interoperability issues prior to proceeding with more rigorous testing and evaluation (T&E).

Information Assurance Range

Implementing the preceding recommendations for requirements, S&T, and architecture establishes a framework to accelerate the certification and accreditation (C&A) process. As architects collaborate with requirements analysts to document capability needs, S&T agents notify vendors using BAAs to articulate associated security specifications. A SIDECAR portal offers industry the same searchable database structure that it provides to requirements managers to communicate evolving needs. This increases the likelihood that COTS offerings will contain pre-approved security mechanisms that meet or exceed the government's standards. The portal also enables better reciprocity of C&A across the DoD.

The model offers another option to compress certification timelines by permitting concurrent T&E for performance characteristics as well as information security. A persistent, virtual environment established by the Defense Information Systems Agency facilitates managing risk associated with information security. This "DoD Information Assurance (IA) Range," achieved initial operational capability in 2010 and "can operate as a stand-alone simulator; or it can interface and interoperate with other ranges run by combatant commands, services, and agencies."[90] The DoD IA Range provides an "operationally realistic environment to include a representation of the IA and computer network defense components deployed on the Global Information Grid."[91]

The IA Range can test, evaluate, and ensure interoperability of Enterprise IA applications and/or configure "virtual enclaves in accordance with specific test requirements."[92] For example,

Vendor X submits Application Y to determine security vulnerabilities in preparation for C&A. This assessment can be made in a virtual, partitioned sector; or it can be evaluated against all previously approved systems in the MCISR-E. In either scenario, communications operate on a closed network without any adverse impact to operational networks.[93] As the IA Range matures and becomes more distributed, it can meet the U.S. CIO's intent to employ cloud computing models to improve security through collaboration from disparate agencies.

Conclusions and Recommendations

A mismatch between the DoD's current acquisition process and the rate of technological change results in the U.S. repeatedly outspending its adversaries at the risk of fielding obsolescent capability. This is particularly true for the non-state actor who freely exploits the commercial sector and successfully harvests the benefits of web-enabled capabilities without bureaucratic delay. Conversely, U.S. military ISR systems fall short in seamlessly linking data across multiple intelligence disciplines (e.g., Human, Signals, and Imagery Intelligence) despite having access to the latest technology. The DoD must implement a separate, agile process for acquiring IT components that comprise the bulk of ISR capability in order to close this gap.

Marine Corps leadership is serious about solving the information synthesis problem with a fundamentally different approach. The MCISR-E is poised to sponsor a pilot program that will demonstrate the value of an improved rapid IT acquisition process. The new process targets existing problem areas including: time, requirements, architecture, security, and cost. A supply-chain model utilizing an incremental, evolutionary approach shortens the time it will take to deliver valued capabilities to warfighters. An ERP offers additional structure to integrate current requirements with emerging ISR needs generated from the bottom-up. Finally, a PLA modeled after commercial best practices provides an agile framework that identifies essential parts, and offers testing to ensure final products function with the important qualities users expect.

The future of MCISR capabilities will be driven by component integration and rapid deployment of new products that enable diverse interaction across the ISR enterprise. A scalable PLA will facilitate the accelerated development of new technologies by combining existing [software] components with innovative products. An active core of stakeholders will continually refine requirements and QAs to ensure they still present credible needs.[94] Using a prototype PISR PLA, the Marines can begin to populate the shelves of a virtual MCISR-E store replete with off-the-shelf capabilities prequalified for procurement and immediately available for deployment. Offerings will gradually expand until the service has populated a virtual Defense Enterprise Mall with ever more capable, pre-approved, COTS capabilities. The Marines are ready to implement emerging policy revisions using ERP, PLA, and an ISIL construct in order to accelerate the delivery of value-added products to its troops deployed on the front lines.

Endnotes

[1] U.S. Defense Science Board Task Force. *Department of Defense Policies and Procedures for the Acquisition of Information Technology.* Washington, D.C. March 2009.

[2] Department of the Navy, Headquarters, Marine Corps, Director of Intelligence. *Marine Corps Intelligence, Surveillance, Reconnaissance-Enterprise Roadmap.* Arlington, VA. April 2010.

[3] Office of the Secretary of Defense, Memorandum for Under Secretary of Defense for Acquisition Technology and Logistics. *Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology.* Arlington, VA: March 2009.

[4] Defense Science Board (DSB), Mar 2009, viii.

[5] Gordon E. Moore, "Cramming More Components onto Integrated Circuits." *Electronics*, Vol 38, no. 8 (April 19, 1965): 1.

[6] Dale W. Jorgenson and Charles W. Wessner. "Measuring and Sustaining the New Economy, Software, Growth, and the Future of the U.S. Economy: Report of a Symposium." *National Research Council*, Fig 1 (2006): 6.

[7] DSB, Mar 2009, ix, 2.

[8] Government Accountability Office, *Better Weapon Program Outcomes Require Discipline, Accountability, and Fundamental Changes in the Acquisition Environment* (Washington, D.C: Government Accountability Office, 2008), 5.

[9] DSB, Mar 2009, 36.

[10] Rick Hayes-Roth, "Executive Redirection to Agile IT Methods: A Proposed Pilot Effort to Radically Improve Time to Value." *Unpublished paper* (Palo Alto, CA, April 2007).

[11] DSB, Mar 2009, x, 56.

[12] Robert Gates, "A Balanced Strategy: Reprogramming the Pentagon for a New Age." *Foreign Affairs* Washington D.C., January/February 2009, 5.

[13] DSB, Mar 2009, xi.

[14] Glen T. Logan, "The Modular Open Systems Approach to Defense Acquisition: OS vis -a-vis OA." August 2007, http://somd-afcea.org/downloads/Logan_ModularOpenSystemsApproach.pdf (accessed 31 January 2011).

[15] Ibid

[16] DSB, Mar 2009, 19, 49.

[17] Software Engineering Institute, "Software Architecture Glossary." http://www.sei.cmu.edu (accessed 11 January 2011).

[18] DSB, Mar 2009, xvii.

[19] Brian Rideout and Andy Strickland, "Military Application of Networking by Touch in Collaborative Planning and Tactical Environments," (Master's Thesis, Naval Postgraduate School, 2007), 51.

[20] Rideout and Strickland, 52

[21] DSB, Mar 2009, 28.

[22] DSB, Mar 2009, 7.

[23] DSB, Mar 2009, 50-52.

[24] DSB, Mar 2009, 2.

[25] Ibid

[26] Defense Acquisition University, "USAF Weapons Systems Software Management Guidebook." August 2008, https://acc.dau.mil/CommunityBrowser.aspx?id=24374&lang=en-US (accessed 18 January 2011).

[27] Defense Acquisition University, "Defense Acquisition Guidebook Dated: August 5, 2010." https://acc.dau.mil/CommunityBrowser.aspx?id=350719 (accessed 18 January 2011).

[28] DSB, Mar 2009, 67.

[29] DSB, Mar 2009, vii, 1.

[30] DSB, Mar 2009, 5.

[31] DSB, Mar 2009, vii, 1.

[32] DSB, Mar 2009, 15, 17.

[33] U.S. Department of Defense Instruction 8510.01. *DoD Information Assurance Certification and Accreditation Process (DIACAP).* Arlington, VA: Department of Defense, November 2007.

[34] DSB, Mar 2009, 14.

[35] Budget of the United States Government: FY 2007. http://www.gpoaccess.gov/usbudget/fy07/index.html (accessed 18 January 2011).

[36] Information Technology Dashboard. http://it.usaspending.gov/?q=portfolios (accessed 18 January 2011).

[37] DSB, Mar 2009, 14.

[38] Software Engineering Institute, "Software Product Lines." http://www.sei.cmu.edu/productlines/ (accessed 4 Feb 2011).

[39] Office of the Secretary of Defense, Report to Congress Pursuant to Section 804 of the National Defense Authorization Act for Fiscal Year 2010. *A New Approach for Delivering Information Capabilities in the Department of Defense.* Arlington, VA: November 2010, 4.

[40] 111th Congress: "Sec. 804. Implementation of New Acquisition Process for Information Technology Systems." P.L. 111-84, The National Defense Authorization Act for Fiscal Year 2010. Washington, D.C.

[41] OSD, *A New Approach,* 16.

[42] Vivek Kundra. *25 Point Implementation Plan to Reform Federal Information Technology Management.* United States Chief Information Officer, Office of Management and Budget, Washington, D.C., December 2010, 11.

[43] OSD, *A New Approach,* 6, 9.

[44] Kundra, *25 Point Implementation,* 11.

[45] OSD, *A New Approach,* 6.

[46] Kundra, *25 Point Implementation,* 31.

[47] Ibid

[48] OSD, *A New Approach,* 4.

[49] Kundra, *25 Point Implementation,* 12.

[50] Charles A. Wells, "Information Technology Requirements Oversight and Management (The "IT" Box)". *Information Paper,* Arlington, VA: J-8 Deputy Director for Resources and Acquisition, April 2010.

[51] OSD, *A New Approach,* 3,15.

[52] OSD, *A New Approach,* 5, 9, 10.

[53] OSD, *A New Approach,* 2.

[54] OSD, *A New Approach,* 10, 12.

[55] Kundra, *25 Point Implementation,* 11.

[56] Kundra, *25 Point Implementation,* 3.

[57] OSD, *A New Approach,* 6.

[58] OSD, *A New Approach,* 5.

[59] OSD, *A New Approach,* 10.

[60] OSD, *A New Approach,* 12.

[61] Eric Knorr and Galen Gruman, "What Cloud Computing Really Means." *InfoWorld.* April 2008, http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,0 (accessed 3 Feb 2011).

[62] Kundra, *25 Point Implementation,* 8.

[63] OSD, *A New Approach,* 18.

[64] OSD, *A New Approach,* 13.

[65] Kundra, *25 Point Implementation,* 7.

[66] Kundra, *25 Point Implementation,* 23.

[67] MCISR-E Roadmap, 1.

[68] Marine Corps Service Campaign Plan 2009-2015, Marine Corps Administrative Message 003/10. January 2010, http://www.usmc.mil/news/messages/Pages/MARADMIN003-10.aspx (accessed 4 Feb 2011).

[69] MCISR-E Roadmap, 10.

[70] MCISR-E Roadmap, 4.

[71] MCISR-E Roadmap, 2.

[72] MCISR-E Roadmap, 4.

[73] MCISR-E Roadmap, 10.

[74] Ibid.

[75] Douglas Lenat, "Automated JCIDS: A Rich, Semantic, Automated, Acquisition Framework." February 2010, http://jcidswiki.cyc.com/index.php5/Main_Page (accessed 7 Feb 2011), 2.

[76] Ibid.

[77] Ibid.

[78] MCISR-E Roadmap, 11.

[79] Office of Naval Research, "ISR Thrust." http://www.onr.navy.mil/About-ONR.aspx (accessed 8 Feb 2011).

[80] Defense Acquisition University, "Technology Readiness Levels." https://acc.dau.mil/CommunityBrowser.aspx?id=24699 (accessed 8 Feb 2011).

[81] OSD, *A New Approach,* 13.

[82] Marine Corps Systems Command, "Persistent ISR Product Line Architecture version 1.0," Monterey, CA (2010).

[83] MCISR-E Roadmap, 19.

[84] MCISR-E Roadmap, 4.

[85] MCSC, PISR PLA 1.0, i.

[86] Ibid.

[87] Customer Relationship Management, "Knowledge Base." http://searchcrm.techtarget.com/definition/knowledge-base (accessed 11 Feb 2011).

[88] SEI Software Architecture Glossary.

[89] Rideout and Strickland, 77.

[90] Defense Systems, "New DoD Test Range Serves as Cyber Training Ground." http://defensesystems.com/Articles/2010/12/01/DOD-Launches-Cyber-Test-Range.aspx?Page=1 (accessed 12 Feb 2011).

[91] Memorandum of Agreement between Defense Information Systems Agency and The United States Marine Corps, March 2010, 1.

[92] Ibid.

[93] Ibid.

[94] Rideout and Strickland, 85
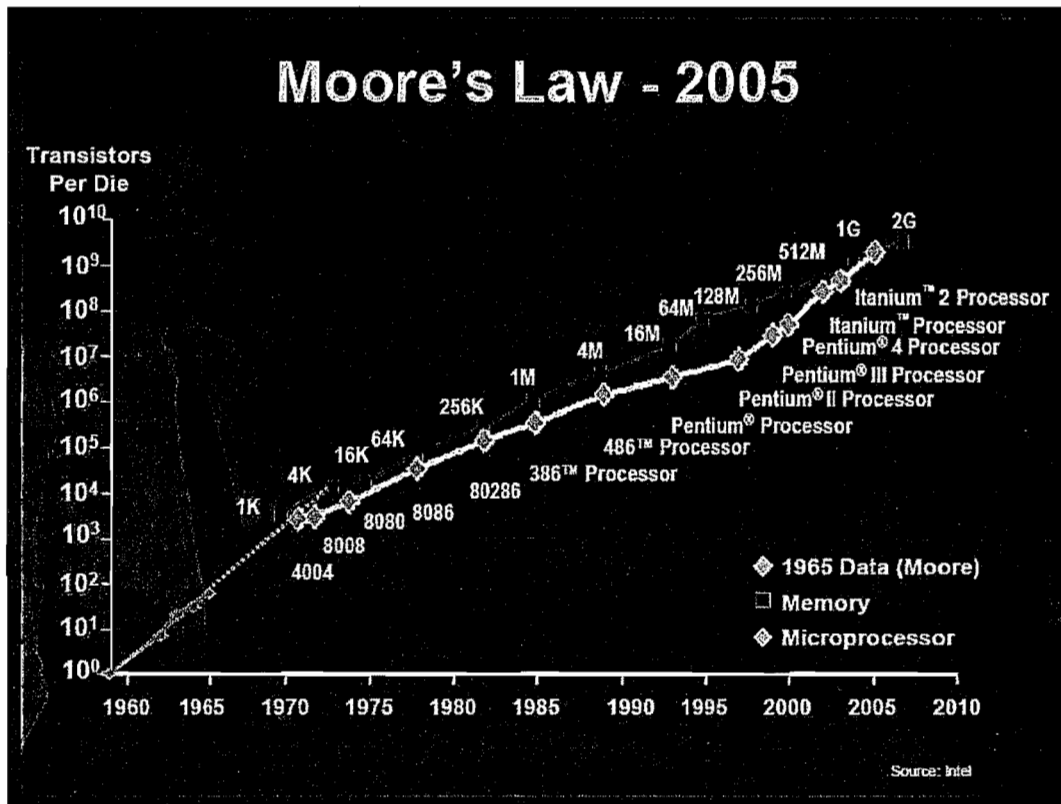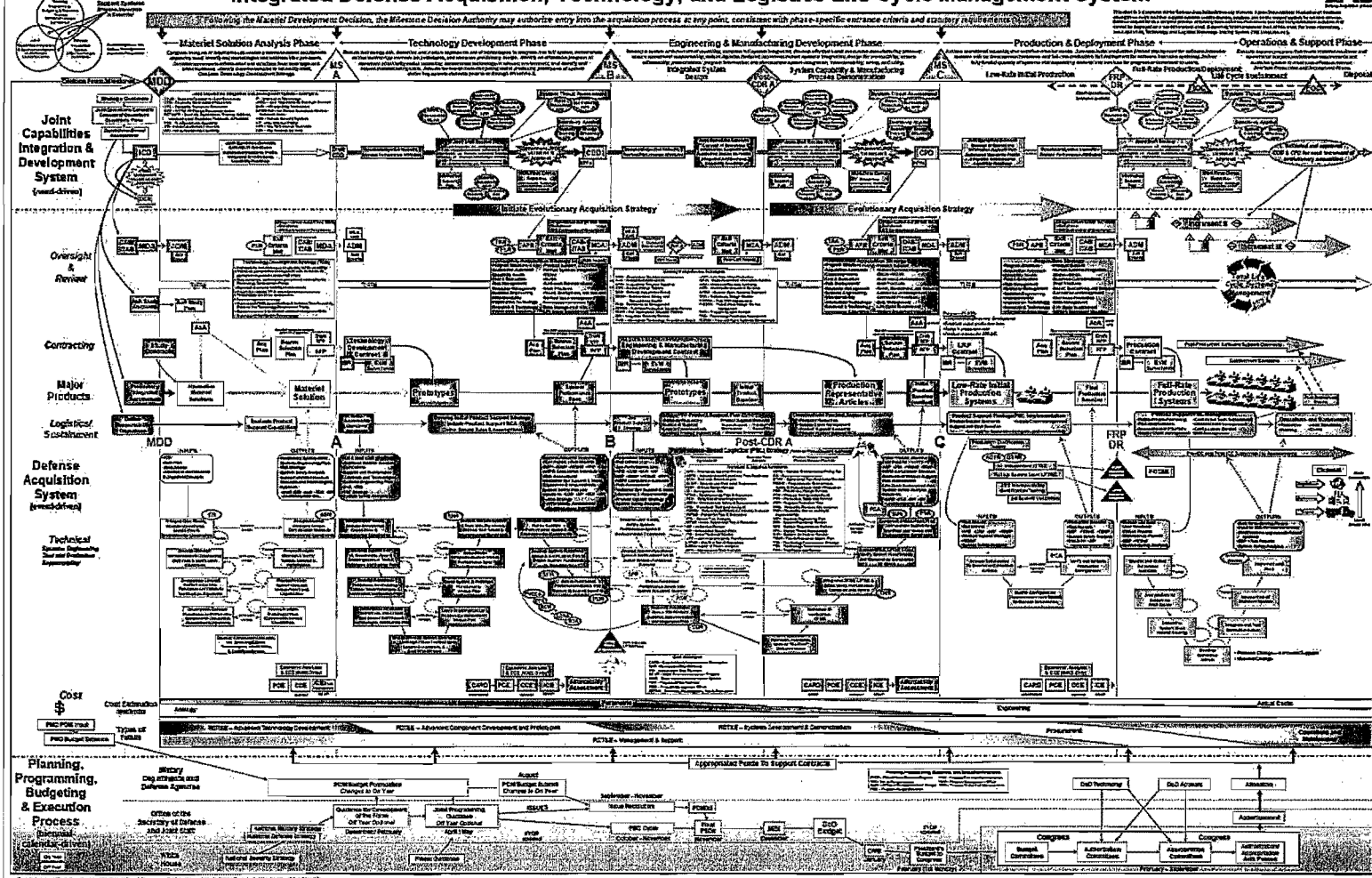
Appendix A: Figures

Figure 1 - Moore's Law Applied to Processing and Memory

(From http://www.victusspiritus.com/2010/07/03/is-there-a-moores-law-for-machine-intelligence/)
Accessed 17 January 2011

Figure 2 - Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System

(From http://www.dau.mil). Accessed 18 January 2011.

The Defense Acquisition University's (DAU) chart depicts the three principle, overlapping DoD decision-making support systems for acquisitions. From top to bottom they include: Joint Capabilities Integration and Development System (JCIDS), Defense Acquisition System (DAS), and Planning, Programming, Budget and Execution (PPB&E). An acquisition starts with JCIDS which employs a lengthy systematic method for assessing gaps in military joint war-fighting capabilities. Solutions are recommended and validated by boards, the highest of which is the Joint Requirements Oversight Council (JROC). The JROC is composed of the Vice Chairman, Joint Chiefs of Staff as well as the Vice Chiefs of each military branch. The DAS consists of a management process for the DoD to acquire, test, field, and dispose of weapons systems and automated information systems. PPB&E represents the DoD's resource determination process used to craft plans and programs that satisfy the National Security Strategy.

SYSTEMIC FAILURE MODES IN CERTIFICATION & ACCREDITATION PRACTICES:

Divergence of Asynchronous Cyclic and Random Behaviors
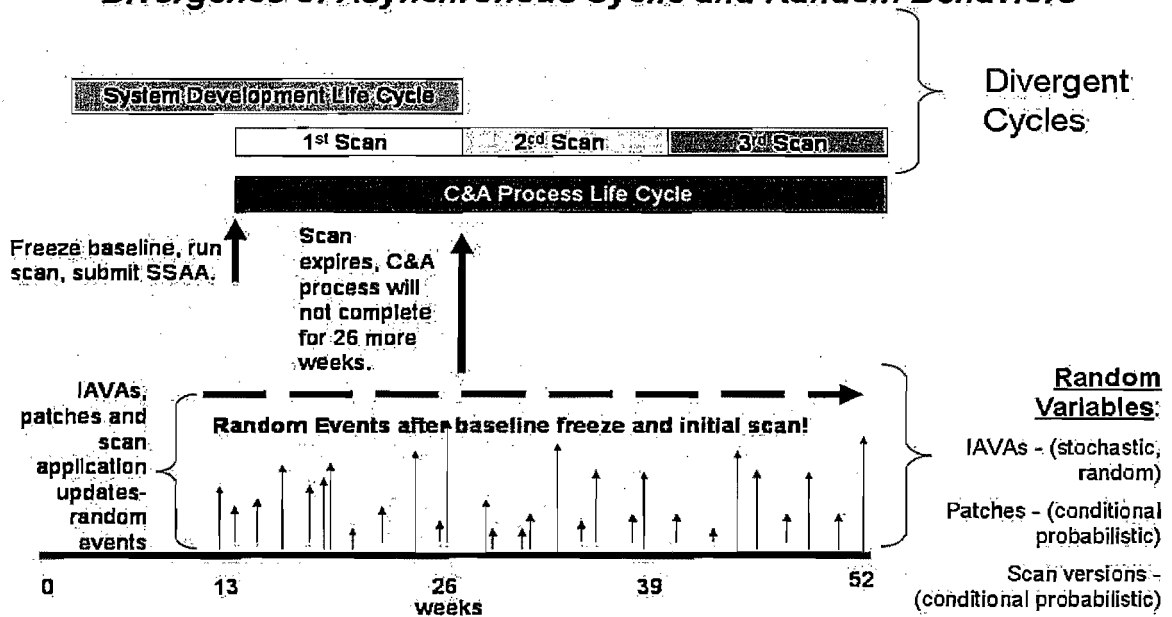
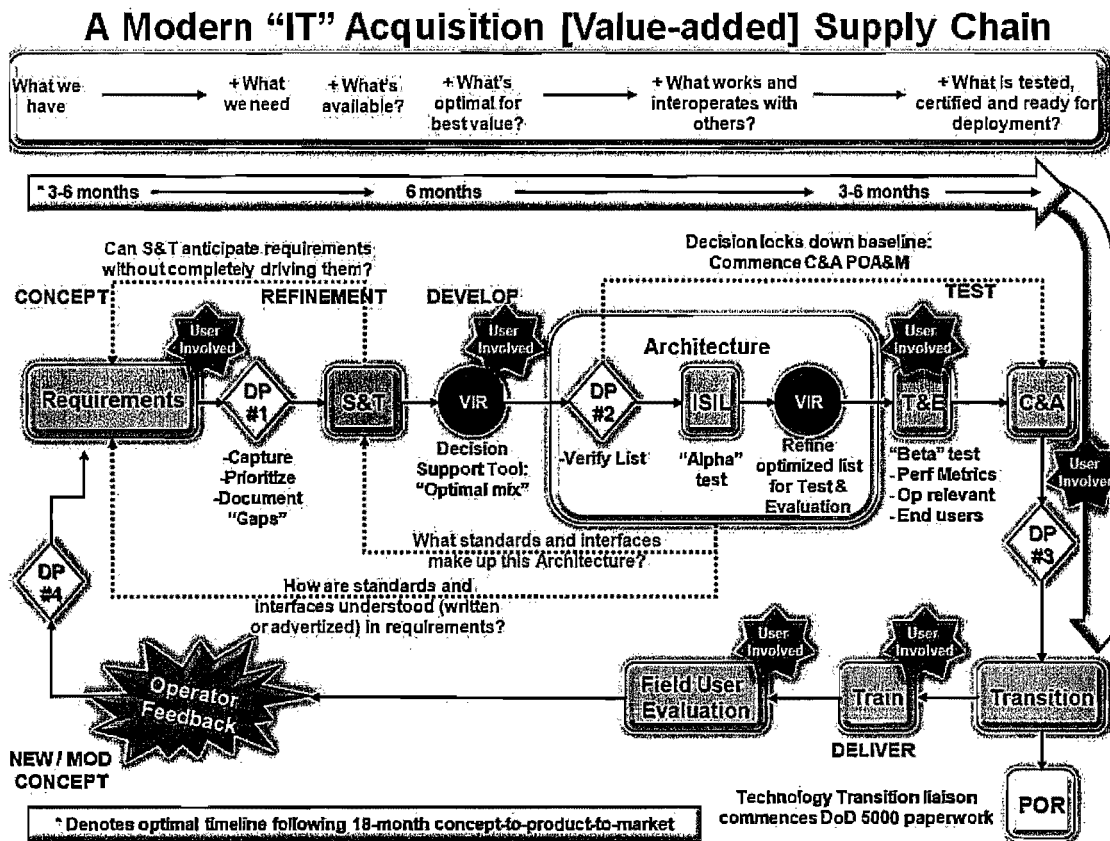**Figure 3 - Asynchronous Cycle and Random Behavior in C&A Process**

(Adapted from: Francis, Michael. *Systemic Failure Modes in Certification and Accreditation Practices: Divergence of Asynchronous Cyclic and Random Behaviors.* White Paper, Quantico, VA., August 2008)

Vulnerabilities are typically discovered by applications that "scan" systems. Vulnerabilities are subsequently assigned severity codes based on assessments performed by certification authorities. Currently, *hard time limits are specified for mitigating the Information Assurance Vulnerability Alerts (IAVA) that stem from these evaluations. While vendors develop and release patches to mitigate mechanisms for vulnerabilities, the scanning applications update their knowledge bases to discover new vulnerabilities in parallel. Often, patches create new, unforeseen vulnerabilities. Thus, the emergence, discovery, and mitigation of vulnerabilities is highly irregular, at best. In short, the dynamic nature of IAVA events contradicts the periodic and deterministic System Development Lifecycle.

In the figure, a vendor completes development of software, locks the baseline from further changes, and submits a System Security Approval Agreement to start the scanning process. The Agreement is reviewed for accreditation with the intent to acquire an Authority to Operate from the Designated Approval Authority. Random events create a cycle of identifying and patching which exceeds the scan's shelf-life. The process resets and repeats. Developers must constantly change system configuration to accommodate the randomly evolving state of scanning, patching, IAVA discovery, and mitigation. Each change and subsequent scan poses risks to schedule, interoperability and integration issues.

*Scan shelf-life equals ninety days.

A Modern "IT" Acquisition [Value-added] Supply Chain

What we have → + What we need + What's available? + What's optimal for best value? → + What works and interoperates with others? → + What is tested, certified and ready for deployment?

* 3-6 months ————→ 6 months ————→ 3-6 months ————→

Can S&T anticipate requirements without completely driving them?

Decision locks down baseline. Commence C&A POA&M

CONCEPT REFINEMENT DEVELOP TEST

User Involved

Architecture

Requirements — DP #1 — S&T — VIR — DP #2 — ISIL — VIR — T&E — C&A

-Capture
-Prioritize
-Document
"Gaps"

Decision Support Tool: "Optimal mix"

-Verify List

"Alpha" test

Refine optimized list for Test & Evaluation

"Beta" test
-Perf Metrics
-Op relevant
-End users

DP #4

DP #3

What standards and interfaces make up this Architecture?

How are standards and interfaces understood (written or advertized) in requirements?

Operator Feedback

NEW / MOD CONCEPT

Field User Evaluation — Train — Transition

DELIVER

* Denotes optimal timeline following 18-month concept-to-product-to-market

Technology Transition liaison commences DoD 5000 paperwork

POR

Figure 4 -Implementing A Modern IT Acquisition Supply Chain

The model offers a framework for a MCISR-E Pilot program to conceive, produce, and deliver valued IT products in eighteen months or less. Design considerations coincide with Section 804 TF and OSD recommendations. These include: (1) early and continual involvement of the user, (2) multiple, rapidly executed increments of capability, (3) early, successive prototyping to support the evolution of IT, and (4) a modular, open-systems approach.

Green blocks represent project entities capable of cross collaboration under an overall Pilot Executive Manager. Solid lines depict process flow; dashed lines indicate parallel work or feedback loops. An Enterprise Requirements Traceability Matrix (not depicted) offers a baseline from which new requirements emerge. Requirements analysis captures, prioritizes, and documents capability gaps. Decision Point (DP) #1 confirms those gaps and establishes prescribed periods for implementing solutions, i.e., increment one, year one, phase one, etc. S&T partners explore alternatives to fulfill gaps. This includes narrowing the field of alternatives, assessing risk, and advising on priorities. Valuing ISR Resources (VIR) consists of an algorithm-based portfolio analysis tool designed to assist with validation and verification of requirements. DP #2 marks an 80% solution or "cut-off" point for a particular increment. Software baselines are frozen in order to proceed with the C&A plan of actions and milestones.

The architecture entity employs a PLA approach that incorporates DP#2, a intelligence system integration laboratory (ISIL), and a second instance of VIR, as needed. Architects focus on compatible interfaces to facilitate system integration and component reuse. Where possible, data standardization is explicitly articulated in documented requirements. The ISIL incorporates "alpha" testing which simulates operational assessment prior to more rigorous T&E. "Beta" testing invites end users to critique capability functionality in a limited but operationally relevant environment. DP #3 matches tested, certified, and approved components with intended customers then transitions the capability to the field as a field user evaluation. DP #4 weighs battlefield performance against emerging requirements.

Appendix B: Tables

Theme	Problem / Challenge	Recommendation
Time	-Adaptations to Moore's Law encompass an array of IT components; the Law remains relevant. -DoD Acquisition process takes too long -DoD IT programs average 21 month delay; cycle time for IT is 91 months (approx 7.5 years). -Commercial sector operates on 6-12 month development cycles.	-Make cycle time to deliver increased value to war-fighters the top priority. -Shorten project initiation timelines; maintain pace with [proven] technology change rates. -Implement incremental cycles of 18 months. -Move from large, multi-year programs to short-duration projects.
Requirements	-Conventional programs seek a 99% solution which takes years to define, agree, and approve. -DoD typically over-defines final requirements with respect to delivering capability increments. -IT requirements are hindered by inadequate communication with industry; program staff and end user communication is often insufficient. -Poorly written specifications result in waste, delays, and the perception that IT investments are not valuable.	-Current missions require 75% solutions determined over a period of months, not years. -Implement enterprise focus across portfolio of capabilities with open, modular approach. -Concentrate on manageable increments that deliver capabilities in shorter time frames. -Define initial objectives then weigh desired capabilities against cost and the ability to reach IOC with the best [available] solutions. -Prioritize increments through iterative reviews and frequent technical assessments. -Early and continual involvement of user.
Architecture	-Definitions are problematic. -Recommendations to pursue various types of architecture lack necessary focus. -Current solutions are stand-alone and paper-based rather than agile and adaptive.	-Employ an evolutionary, PLA approach; create a persistent plug-and-play IT platform. -Maximize efficient component reuse; enable time-to-value improvements across an enterprise. -Seize opportunities to identify and address system interoperability issues; employ early, successive prototyping with end users. -Integrate new technologies as they become available to support development.
Leadership and Policy	-Well-intentioned policies suffer misinformed interpretations preventing Program Managers from delivering valued results on time. -Extant policies support "one-size-fits-all" despite knowledge of technology trends. -Senior leaders lack technical experience. -The acquisition process is too bureaucratic.	-Implement a unique IT acquisition system. -New policies require new models with corresponding incentives. -Put more accountability on timely coordination and agile decision cycles through increased stakeholder involvement and frequent in-progress reviews.
Security	-DIACAP (DoDI 8510.01) process levies strict risk management approach to acquire an authority to operate. -Current procedures add over one year to the C&A process widening the gap between the availability of latest IT capabilities and the DoD's ability to certify them.	-Establish test infrastructure in a persistent, virtual, service-based environment. -Integrate security with performance testing to mitigate interoperability issues. -Employ cloud computing to facilitate improving security through collaborative contribution and consumption from disparate agencies.
Cost	-Often considered as a separate variable. -Maintaining annual cost of DoD software-enabled capabilities equals ten times the cost of commercial software industry. -Budgets are driven by calendars, not events.	-Employ a formula that places cost in the context of time and the value of end product(s). -Adopt flexible budget models to support modular development; delegate fiscal decisions to the point of execution; fully embrace COTS technology.

Table 1 - Summary of DSB, DoD, and OMB Findings and Recommendations

Bibliography

Assistant Secretary of the Navy Research, Development and Acquisition Memorandum. *Rapid Acquisition Processing Update.* Arlington, VA: Department of Defense, August 2007.

Bordetsky, Alex and David Netzer. *Testbed for Tactical Networking and Collaboration.* The International C2 Journal, Vol. 4, Number 3, 2010.

Chairman of the Joint Chiefs of Staff Instruction 3470.01. *Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution.* Arlington, VA: Department of Defense, July 2005.

Christensen, Clayton M. *The Innovator's Dilemma.* Harvard Business School Press, 1997.

Customer Relationship Management, "Knowledge Base." http://searchcrm.techtarget.com/definition/knowledge-base (accessed 11 Feb 2011) .

Defense Acquisition University, "Defense Acquisition Guidebook Dated: August 5, 2010." https://acc.dau.mil/CommunityBrowser.aspx?id=350719 (accessed 18 January 2011).

Defense Acquisition University, "Technology Readiness Levels." https://acc.dau.mil/CommunityBrowser.aspx?id=24699 (accessed 8 Feb 2011).

Defense Acquisitions University, "United States Air Force Weapons Systems Software Management Guidebook." Ver 1., 15 August 2008, https://acc.dau.mil/CommunityBrowser.aspx?id=24374&lang=en-US (accessed 18 January 2011).

Defense Systems, "New DoD Test Range Serves as Cyber Training Ground." http://defensesystems.com/Articles/2010/12/01/DOD-Launches-Cyber-Test-Range.aspx?Page=1 (accessed 12 Feb 2011).

Fein, Geoff. "Study Recommends Processes for DoD to Implement Improved IT Acquisition." *Defense Daily* (August 5, 2010): 2-4.

Ferrel, Tyrone H. "Rapid, Value-Based, Evolutionary Acquisition and its Application to a USMC Tactical Service Oriented Architecture." Master's thesis, Naval Postgraduate School, 2009.

Francis, Michael. *Systemic Failure Modes in Certification and Accreditation Practices: Divergence of Asynchronous Cyclic and Random Behaviors*. White Paper, Quantico, VA., August 2008.

Gates, Robert. " A Balanced Strategy: Reprogramming the Pentagon for a New Age." *Foreign Affairs* (January/February 2009).

Gunderson, Chris. *Business Case for Naval ISR Rapid Evolutionary Acquisition (NI-REA)*. September 13, 2010.

Gunderson, Chris. *Let's Cure Defense Enterprise Information Technology Acquisition with a Dose of its Own Medicine*. http://c4i.gmu.edu/events/reviews/2010/papers/Gunderson_Lets_Cure.pdf (accessed Oct 27, 2010).

Gunderson, Chris. *Value Based Acquisition: An Evolutionary, Enterprise, Netcentric Business Model*. World Wide Consortium for the Grid: Government/Industry Partnership for Netcentric Engineering, January 2010.

Gunderson, Chris and Tod Levitt. *Valuing ISR Resources*. Unpublished paper. Washington, D.C., December 2010.

Gunderson, Chris and David Minton. *Coalition Warfare Interoperability Demonstration 2008 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2*. http://c4i.gmu.edu/events/reviews/2009/papers/Gunderson-paper.pdf (accessed Oct 27, 2010).

Hayes-Roth, Rick. "Executive Redirection to Agile IT Methods: A Proposed Pilot Effort to Radically Improve Time to Value." Unpublished paper. Palo Alto, CA, April 2007.

Headquarters, Marine Corps, Director of Intelligence. *Marine Corps Intelligence, Surveillance, Reconnaissance-Enterprise Roadmap*. Arlington, VA: Department of the Navy: April 2010.

Headquarters, Marine Corps, Commandant of the Marine Corps. *Marine Corps Service Campaign Plan 2009-2015*. Administrative Message 003/10. January 2010, http://www.usmc.mil/news/messages/Pages/MARADMIN003-10.aspx (accessed 4 Feb 2011).

Jorgenson, Dale W. and Charles W. Wessner. *Measuring and Sustaining the New Economy, Software, Growth, and the Future of the U.S Economy: Report of a Symposium*. National Research Council. Figure 1, p. 6. 2006. www.nap.edu/catalog/11587.html (accessed 10 Jan 2011).

Knorr, Eric and Galen Gruman. *What Cloud Computing Really Means*. InfoWorld, April 2008. http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031 (accessed 3 Feb 2011).

Kundra, Vivek. *25 Point Implementation Plan to Reform Federal Information Technology Management*. United States Chief Information Officer, Office of Management and Budget, Washington, D.C., December 9, 2010.

Langston, Marv. *Our Military Wave 3 Information Capability is Hostage to Current Wave 2 Bureaucratic Processes – We Can't Get There Without Radical Change*. http://smart-future.org/2009/10/wave-3-dilemma/ (accessed Oct 27, 2010).

Lenat, Douglas. *Automated JCIDS: A Rich Semantic, Automated, Acquisition Framework*. February 2010, http://jcidswiki.cyc.com/index.php5/Main_Page (accessed 7 Feb 2011).

Logan, Glen T. *The Modular Open Systems Approach to Defense Acquisition: OS vis-a-vis OA*. August 2007, http://somd-afcea.org/downloads/Logan_ModularOpenSystemsApproach.pdf (accessed 31 January 2011).

Marine Corps Systems Command, "Persistent ISR Product Line Architecture version 1.0," Monterey, CA, (2010).

Memorandum of Agreement between Defense Information Systems Agency and United States Marine Corps, March 2010.

Moore, Gordon E. *Cramming More Components onto Integrated Circuits*. Electronics, Vol. 38, No 8, April 19, 1965. http://web.eng.fiu.edu/npala/EEE6397/Gordon_Moore_1965_Article.pdf (accessed 10 Jan 2011).

Office of Naval Research, "ISR Thrust." http://www.onr.navy.mil/About-ONR.aspx (accessed 8 Feb 2011).

Office of the Secretary of Defense, Acquisition Technology and Logistics Memorandum for Acquisition Professionals. *Better Buying Power: Guidance for Obtaining Greater Efficiency and Productivity in Defense Spending*. Arlington, VA: September 14, 2010.

Office of the Secretary of Defense, Acquisition Technology and Logistics Memorandum for Acquisition Professionals. *Better Buying Power: Mandate for Restoring Affordability and Productivity in Defense Spending*. Arlington, VA: June 28, 2010.

Office of the Secretary of Defense, Acquisition Technology and Logistics Memorandum for Director, Defense Procurement & Acquisition Policy. *Implementation Directive for Better Buying Power – Restoring Affordability and Productivity in Defense Spending.* Arlington, VA: September 14, 2010.

Office of the Secretary of Defense, Memorandum for Under Secretary of Defense for Acquisition Technology and Logistics. *Final Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology.* Arlington, VA: March 2009.

Office of the Secretary of Defense, Report to Congress Pursuant to Section 804 of the National Defense Authorization Act for Fiscal Year 2010. *A New Approach for Delivering Information Capabilities in the Department of Defense.* Arlington, VA: November 2010.

Rideout, Brian T. and Andy Strickland. "Military Application of Networking by Touch in Collaborative Planning and Tactical Environments." Master's thesis. Naval Postgraduate School, 2007.

Software Engineering Institute. "Software Architecture Glossary." http://www.sei.cmu.edu/ (accessed January 11, 2011).

Software Engineering Institute. "Software Product Lines." http://www.sei.cmu.edu/productlines/ (accessed February 4, 2011).

U.S. Congress: "Sec. 804. Implementation of New Acquisition Process for Information Technology Systems." P.L. 111-84, The National Defense Authorization Act for Fiscal Year 2010. Washington, D.C.

U.S. Defense Science Board Task Force. *Department of Defense Policies and Procedures for Acquisition of Information Technology.* Washington, D.C. March 2009.

U.S. Defense Science Board Task Force. *Fulfillment of Urgent Operational Needs.* Washington, D.C. July 2009.

U.S. Department of Defense 8320.02-G. *Guidance for Implementing Net-Centric Data Sharing.* Arlington, VA: Department of Defense, April 2006.

U.S. Department of Defense 8570.01-M. *Information Assurance Workforce Improvement Program.* Arlington, VA: Department of Defense, May 2008.

U.S. Department of Defense Directive 4630.05. *Interoperability and Supportability of Information Technology and National Security Systems.* Arlington, VA: Department of Defense, April 2007.

U.S. Department of Defense Directive 8115.01. *Information Technology Portfolio Management.* Arlington, VA: Department of Defense, October 2005.

U.S. Department of Defense Directive 8320.02. *Data Sharing in a Net-Centric Department of Defense.* Arlington, VA: Department of Defense, April 2007.

U.S. Department of Defense Inspector General Report D-2010-028. *Rapid Acquisition and Fielding of Material Solutions by the Navy.* Arlington, VA: Department of Defense, Dec 2009.

U.S. Department of Defense Instruction 8510.01. *DoD Information Assurance Certification and Accreditation Process (DIACAP).* Arlington, VA: Department of Defense, November 2007.

U.S. Department of Defense Memorandum. *DoD Net-Centric Data Strategy.* Arlington, VA: Department of Defense, May 2003.

U.S. Department of the Navy Memorandum. *Department of the Navy Chief Information Officer Memorandum 01-09, Information Assurance Policy for Platform Information Technology.* Arlington, VA: Department of Defense, January 2009.

U.S. Government Accounting Office. *Better Weapon Program Outcomes Require Discipline, Accountability, and Fundamental Changes in the Acquisition Environment.* Washington, D.C., GAO-08-782, June 3, 2008.

U.S. Government Accounting Office. *Intelligence, Surveillance, and Reconnaissance: Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development.* Washington, D.C., Government Accountability Office, April 19, 2007.

Wells, Charles A. *Information Paper: Information Technology Requirements Oversight and Management (The "IT" Box).* Arlington, VA: Department of Defense, J-8 Deputy Director for Resources and Acquisition, April 2010.